GLOSSARY OF TERMS

Adware: Any software application which displays advertising banners while the program is running. The authors include additional code, which can be viewed through pop-up windows or through a bar that appears on the computer screen. Adware has been criticized because it usually includes code that tracks a user's personal information and passes it on to third parties, without the user's authorization or knowledge.

Cookie: Cookies are pieces of information generated by a Web server and stored in the user's computer, ready for future access. Cookies are embedded in the HTML information flowing back and forth between the user's computer and the servers. Cookies were implemented to allow user-side customization of Web information.

Firewall: A firewall is a hardware or software solution to enforce security policies. In the physical security analogy, a firewall is equivalent to a door lock on a perimeter door or on a door to a room inside of the building — it permits only authorized users such as those with a key or access card to enter. A firewall has built-in filters that can disallow unauthorized or potentially dangerous material from entering the system. It also logs attempted intrusions.

Phishing: Where a perpetrator sends out legitimate-looking emails appearing to come from some of the Web's biggest site, including, but not limited to eBay, PayPal, MSN, in an effort to phish (pronounced "fish") for personal and financial information from a recipient.

Spoofing: A technique in which a fraudster pretends via email or Web site to be someone else. This is typically done by copying the content of a legitimate Web site to a fake Web site.

Spyware: Any software using someone's Internet connection in the background without their knowledge or explicit permission. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else.

Trojan Horse: A malicious or harmful code contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk.

Virus: Self-replicating, malicious code that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence.

Worm: Independent program that replicates from machine to machine across network connections often clogging networks and information systems as it spreads.